



BestScoreSheet Q&A Demo

Cisco 642-523

Securing Networks with PIX and ASA

1. Which of these commands enables the DHCP server on the DMZ interface of the Cisco ASA with an address pool of 10.0.1.100-10.0.1.108 and a DNS server of 192.168.1.2?

A. dhcpd address 10.0.1.100-10.0.1.108 DMZ

dhcpd dns 192.168.1.2 dhcpd enable DMZ

B. dhcpd range 10.0.1.100-10.0.1.108 DMZ

dhcpd dns server 192.168.1.2 dhcpd DMZ

C. dhcpd address range 10.0.1.100-10.0.1.108

dhcpd dns 192.168.1.2 dhcpd enable

D. dhcpd address range 10.0.1.100-10.0.1.108

dhcpd dns server 192.168.1.2 dhcpd enable DMZ

Answer: A

2. Refer to the exhibit. Based on this output, which of the following statements is true?

```
asa1(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
  alert-interval 300
access-list ACLOUT; 4 elements
access-list ACLOUT line 1 extended permit tcp 192.168.6.0 255.255.255.0 host
  192.168.1.11 eq www (hitcnt=4) 0x984ebd70
access-list ACLOUT line 2 extended permit tcp host 192.168.6.10 host 192.168.1.11 eq
  ftp (hitcnt=1) 0x53490ecd
access-list ACLOUT line 3 extended permit tcp any host 192.168.1.9 eq www (hitcnt=8)
  0x83af39ca
access-list ACLOUT line 4 extended deny ip any any (hitcnt=4) 0x2ca30385
access-list ICMPDMZ; 1 elements
access-list ICMPDMZ line 1 extended permit icmp host bastionhost any echo-reply
  (hitcnt=12) 0xabc4532d
access-list ACLIN; 1 elements
access-list ACLIN line 1 extended permit tcp any host 192.168.6.10 eq www
  (hitcnt=19) 0x4dac763f
```

A. The ACLOUT access list has been designed to allow the IP address with the network address of 192.168.6.0 to have unrestricted access to the web server at IP address 192.168.1.11.

B. The ACLIN access list permits web access from host 192.168.6.10 to all hosts behind the Cisco ASA.

C. The ICMPDMZ access list denies all ICMP traffic bound for the bastion host except echo replies

D. The ACLOUT access list has been designed to deny the IP address 192.168.1.11 web access to the host with a network address of 192.168.6.0.

Answer: A

3. Which mode of operation must you enter in order to recover the Cisco ASA password?

A. unprivileged

B. privileged

C. configure

D. monitor

Answer: D

4. Which command both verifies that NAT is working properly and displays active NAT translations?

- A. show running-configuration nat
- B. show nat translation
- C. show xlate
- D. show ip nat all

Answer: C

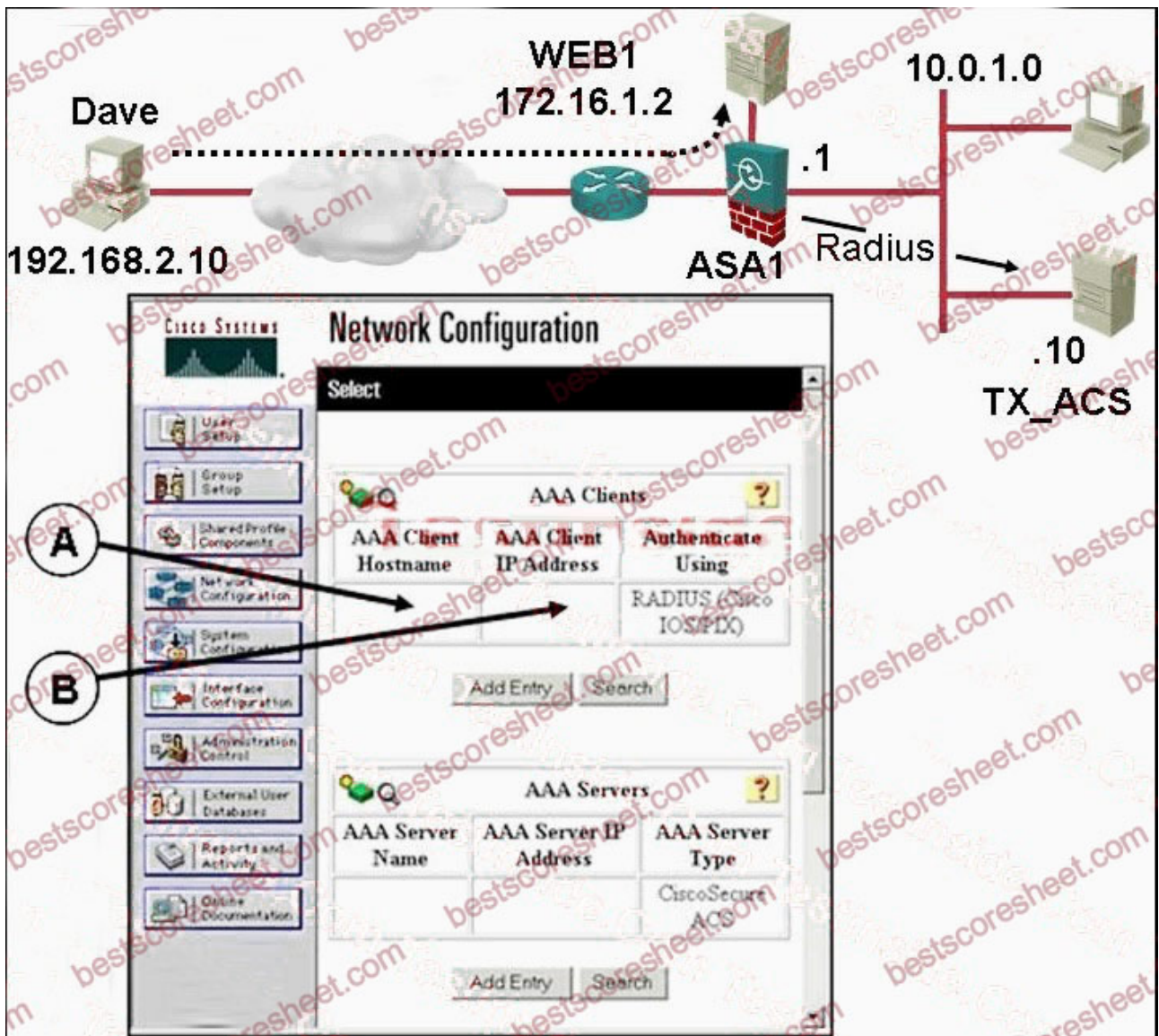
5. The Cisco VPN Client supports which three of these tunneling protocols and methods? (Choose three.)

- A. IPsec over TCP
- B. IPsec over UDP
- C. ESP
- D. AH
- E. SCEP
- F. LZS

Answer: ABC

6. Refer to the exhibit. A network administrator wants to authenticate remote users who are accessing the WEB1 server from the Internet. When a remote user initiates a session to the WEB1 server, the ASA1 security appliance will verify the user's credentials with the TX_ACS AAA server via RADIUS. To accomplish this, the administrator must load and configure Cisco ACS software on the TX_ACS AAA server. During the process, the administrator must correctly configure the AAA client information in the Cisco ACS network configuration window.

What must the administrator place in field A (AAA Client Hostname) and field B (AAA Client IP address)?



- A. AX_ACS
 - B?0.0.1.10
 - B. AEB1
 - B?72.16.1.2
 - C. Aave
 - B?92.168.2.10
 - D. ASA1
 - B?0.0.1.1
- Answer: D

7. When configuring a crypto ipsec transform-set command, how many unique transforms can a single transform set contain?
- A. one
 - B. two
 - C. three
 - D. four

Answer: B

8. Refer to the exhibit. An administrator is adding descriptions to class maps for each part of the modular policy framework. What text would the administrator add to the description command to describe the TO_SERVER class map?

```
asa1(config)# access-list UDP permit udp any any
asa1(config)# access-list TCP permit tcp any any
asa1(config)# access-list PUBLIC_WEB permit ip any 10.10.10.100 255.255.255.255

asa1(config)# class-map ALL_UDP
asa1(config-cmap)# description "This class-map matches all UDP traffic"
asa1(config-cmap)# match access-list UDP

asa1(config-cmap)# class-map ALL_TCP
asa1(config-cmap)# description "This class-map matches all TCP traffic"
asa1(config-cmap)# match access-list TCP

asa1(config-cmap)# class-map ALL_WEB_SERVER
asa1(config-cmap)# description "This class-map matches all HTTP traffic"
asa1(config-cmap)# match port tcp eq http

asa1(config-cmap)# class-map TO_SERVER
asa1(config-cmap)# match access-list PUBLIC_WEB
```

- A. description "This class-map matches all HTTP traffic for the public web server."
- B. description "This class-map matches all HTTPS traffic for the public web server."
- C. description "This class-map matches all TCP traffic for the public web server."
- D. description "This class-map matches all IP traffic for the public web server."

Answer: D

9. Which three of these are potential groups of users for WebVPN? (Choose three.)

- A. employees accessing specific internal applications from desktops and laptops not managed by IT
- B. administrators who need to manage servers and networking equipment
- C. employees that only need occasional corporate access to a few applications
- D. employees that need access to a wide range of corporate applications
- E. users of a customer service kiosk placed in a retail store
- F. remote employees that need daily access to the internal corporate network

Answer: ACE

10. Which of these commands will provide detailed information about the crypto map configurations of a Cisco

ASA?

- A. show run ipsec sa
- B. show ipsec sa
- C. show crypto map
- D. show run crypto map

Answer: D

11. Which of these commands would block all SIP INVITE packets, such as calling-party and request-method, from specific SIP endpoints?

- A. Group the match commands in a SIP inspection policy map.
- B. Group the match commands in a SIP inspection class map.
- C. Use the match calling-party command in a class map. Apply the class map to a policy map that contains the match request-methods command.
- D. Use the match request-methods command in an inspection class map. Apply the inspection class map to an inspection policy map that contains the match calling-party command.
- E. Group the match commands in the global_policy policy map.

Answer: B

12. The primary adaptive security appliance failed, so the secondary adaptive security appliance was automatically activated. The network administrator then fixed the problem. Now the administrator wants to return the primary to "active" status.

Which of these commands, when issued on the primary adaptive security appliance, will reactivate the primary adaptive security appliance and restore it to "active" status?

- A. failover primary active
- B. failover secondary group 1
- C. failover active group 1
- D. failover secondary standby group 1

Answer: C

13. You are configuring a crypto map. Which of these commands would you use to specify the peer to which IPsec-protected traffic can be forwarded?

- A. crypto map set peer 192.168.7.2
- B. crypto map 20 set-peer insidehost
- C. crypto-map policy 10 set 192.168.7.2
- D. crypto map peer7 10 set peer 192.168.7.2

Answer: D

14. Which three types of information can be found in the syslog output for an adaptive security appliance? (Choose three.)

- A. time stamp and date
- B. logging level
- C. default router
- D. interface packet received
- E. hostname of the packet sender
- F. message text

Answer: ABF

15. With adaptive security appliance code of version 7.0 or later, which three hardware and software requirements must be met before failover can be configured? (Choose three.)

- A. The adaptive security appliances must be the same type of platform.
- B. RAM, flash, modules, and interfaces must be identical on each unit.
- C. The failover pair must meet hardware and software requirements, but can be a PIX and a Cisco ASA.
- D. Only RAM and interfaces must be identical on each unit.
- E. Major and minor software releases must match, but software versions do not need to be identical.
- F. Software versions must have the same major release version, but minor release versions do not need to match.

Answer: ABE

16. Which three of these are encryption algorithms used by Cisco ASA security appliances? (Choose three.)

- A. DES
- B. Blowfish
- C. RC4
- D. 3DES
- E. AES
- F. Diffie-Hellman Group 5

Answer: ADE

17. Which command configures the Cisco ASA console for SSH access by a local user?

- A. aaa authentication ssh console LOCAL
- B. ssh console username sysadmin password cisco123
- C. ssh username sysadmin password cisco123
- D. aaa authentication ssh LOCAL

Answer: A

18. Which of the following statements about adaptive security appliance failover is true?

- A. The Cisco ASA and PIX security appliances support LAN-based and cable-based failover.
- B. The Cisco ASA security appliance only supports cable-based failover.
- C. The PIX adaptive security appliance only supports LAN-based failover.
- D. The PIX adaptive security appliance supports LAN-based and cable-based failover.

Answer: D

19. Which of these commands enables IKE on the outside interface?

- A. ike enable outside
- B. nameif outside isakmp enable
- C. isakmp enable outside
- D. int g0/0 ike enable (outbound)

Answer: C

20. Which of the following statements about the configuration of WebVPN on the Cisco ASA is true for Cisco ASA version 7.2?

- A. WebVPN and Cisco ASDM can both be enabled on the same interface, but must run on different TCP ports.
- B. WebVPN and Cisco ASDM cannot be enabled at the same time on the Cisco ASA.
- C. WebVPN and Cisco ASDM can only be enabled at the same time using the command line interface.
- D. WebVPN and Cisco ASDM cannot run on the same interface.

Answer: A